IN THE CLAIMS

1. (Currently Amended) A method for transporting encrypted media, comprising:

receiving a request to transport encrypted Internet Protocol (IP) media packets over a circuit switched network;

establishing an IP link over the circuit switched network; ~~and~~

receiving encrypted IP media packets corresponding to the request, the encrypted IP media packets having encrypted layer four transport layer headers and layer three network layer headers;

replacing the existing layer three network layer headers with locally generated layer three network layer headers independently of the encrypted layer four transport layer headers and without replacing the encrypted layer four headers such that encryption protecting the layer four headers and corresponding encompassed payloads is preserved and not locally decrypted; and

transporting the revised encrypted IP media packets over the IP link established over the circuit switched network.

2. (Original) A method according to claim 1 including establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link.

3. (Original) The method according to claim 2 including establishing the data channel over an Integrated Services Digital Network (ISDN) channel of a Public Services Telephone Network.

4. (Currently Amended) A method according to claim 1 including transporting the revised encrypted IP media packets over [[the]] a packet switched network without decrypting or decoding the media that includes voice data ~~in the encrypted IP media packets~~.

5. (Currently Amended) A method according to claim 1 including:

receiving call requests from endpoints connected to a [[the]] packet switched network;

identifying the call requests that require IP encryption;

identifying ingress devices in the circuit switched network associated with the identified call requests that support transport of the encrypted IP media packets over the circuit switched network;

establishing IP links over the circuit switched network with the identified ingress ~~egress~~ devices; and

transporting the revised encrypted IP media packets to the identified ingress devices.

6. (Currently Amended) A method according to claim 5 including:

identifying non-supporting ingress devices in the circuit switched network associated with the identified call requests that do not support transport of encrypted IP media packets over the circuit switched network;

establishing circuit switched connections over the circuit switched network for the identified non-supporting egress devices;

decrypting and decoding media in the encrypted IP media packets associated with the non-supporting ingress ~~egress~~ devices; and

re-encoding and re-encrypting the media into a circuit switched network format; and

transporting the re-encoded and re-encrypted media over the circuit switched connections to the non-supporting egress devices.

7. (Currently Amended) A method according to claim 1 including:

authenticating an ingress device associated with the IP media packets;

sending a first encrypted key associated with a first endpoint over the circuit switched network to the authenticated ingress device;

receiving a second encrypted key over the circuit switched network from the authenticated ingress device associated with a second endpoint;

decrypting the second key and forwarding the decrypted second key over a [[the]] packet switched network to the first endpoint;

encrypting media at the first endpoint directed to the second endpoint using the first key; and

decrypting the revised encrypted IP media packets at the first endpoint received from the second endpoint using the second key.

8. (Original) A method according to claim 1 including encrypting the IP media packets only once at a first sending endpoint and decrypting the IP media packets only once at a receiving second endpoint.

9. (Original) A method according to claim 1 including:

encrypting the IP media packets using a Secure Real-time Transport Protocol (SRTP);

establishing a Point to Point Protocol (PPP) connection over an Integrated Services Digital Network(ISDN) channel in the circuit switched network; and

sending the SRTP encrypted IP media packets over the PPP connection.

10. (Original) A network processing device, comprising:

a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network, the processor forwarding packets having an encrypted IP packet payload between the two endpoints without decrypting the encrypted IP packet payload when transferred between the IP network and circuit switched network.

11. (Original) A network processing device according to claim 10 wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link.

12. (Currently Amended) A network processing device according to claim 10 wherein the processor selects a first codec when forwarding other IP packet payloads that are ~~the encrypted IP packet payload is~~ decrypted for transport over a PSTN connection in the circuit switched network and selects a second codec with higher compression than the first codec when the encrypted IP packet payload is not decrypted and transported over a data link in the circuit switched network.

13. (Original) A network processing device according to claim 10 including a memory containing a dial plan for identifying phone numbers that can be transferred between the IP network and the circuit switched network without decrypting the encrypted IP packet payload.

14. (Original) A network processing device according to claim 10 including memory for storing a shared key shared with an ingress device located at an ingress side of the IP network, the processor receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the ingress device.

15. (Currently Amended) A network processing device according to claim 14 wherein the processor receives a second encrypted key from the ingress device, the processor decrypting the second encrypted key using the shared key and then forwarding the second decrypted key to the first endpoint.

16. (Original) A network processing device according to claim 10 wherein the processor conducts a Point to Point Protocol over an Integrated Services Digital Network (ISDN) channel for establishing an IP link over the circuit switched network and then forwards Secure Real-time Transport Protocol (SRTP) encrypted IP packet payloads over the IP link.

17. (Currently Amended) A method for transporting encrypted media, comprising:

receiving call requests from endpoints;

identifying call requests requiring media encryption;

directing endpoints for the identified call requests to encrypt media using an Internet Protocol(IP) encryption protocol;

identifying the call requests that also require connections over a Public Services Telephone Network(PSTN);

establishing data links over the PSTN for the identified call requests;

receiving encrypted packets corresponding to the IP encrypted media from the endpoints for the identified call requests, the encrypted packets having encryption on a transport layer four header that does not encrypt a lower layer header; ~~and~~

formatting the lower layer header while preserving the encryption on the transport layer four header; and

forwarding the formatted IP encrypted media over the data links established on the PSTN.

18. (Original) The method according to claim 17 including:

authenticating the identified call requests with ingress gateways;

conducting Point-to-Point Protocol (PPP) sessions with the ingress gateways when the ingress gateways are authenticated; and

exchanging encryption keys with the ingress gateways during the PPP session.

19. (Original) The method according to claim 18 including:

encrypting the encryption keys using keys shared with the ingress gateways; and

sending the encrypted encryption key to the ingress gateways.

20. (New) An apparatus, comprising:

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

receive packets over a packet switched network, the packets having first and second headers excluded from encryption for a third header and a payload;

format the first and second headers without decrypting the encryption for the third header and the payload such that the third header and the payload remain encrypted during transfer between the endpoints;

establish a connection over a circuit switched network to a remote network device; and

send the packets having the formatted first and second headers and the encrypted third header and payload on the connection over the circuit switched network.

21. (New) The apparatus of claim 20 wherein the first header is according to the Internet Protocol (IP), the second header is according to the User Datagram Protocol (UDP) and the third header is according to a secure real-time protocol.

22. (New) The apparatus of claim 20 wherein the encrypted payload includes voice data such that the voice data is securely transported across both the circuit switched network and the packet switched network without intermediary decryption.

23. (New) The network processing device of claim 10 wherein the processor is further configured to:

identify one or more network layer headers included in the packets;

remove the network layer headers while preserving encryption on one or more transport layer headers and a corresponding payload;

locally generate one or more new network layer headers;

attach the generated headers to the encrypted transport layer headers and the encrypted corresponding payload; and

forward the packets having the locally generated headers, the encrypted transport layer headers and the encrypted corresponding payload over the connection.

24. (New) The network processing device according to claim 10 where the processor is further configured to:

receive a pre-configuring out-of-band communication that provides a secret that is shared with a remote gateway located between the circuit switched network and the packet switched network;

receive a first key sent from a calling endpoint and usable for decrypting the encrypted IP packet payload;

encrypt the first key using the secret;

send the encrypted first key to the remote gateway;

receive a second key that corresponds to a value stored on a called endpoint and that is encrypted by the remote gateway using the secret;

decrypt the received encrypted second key using the secret; and

send the decrypted second key to the calling endpoint.